APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Computer Hacking Forensic Investigator Training

EC-Council Authorized Training · Applied Technology Academy

EC-Council's Certified Hacking Forensic Investigator (C|HFI) is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around Dark Web, IoT, and Cloud Forensics. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**None with official training (2 yrs InfoSec for exam-only route)**	**$117,950**	**Yes**

Course Overview

The program will help fortify the application knowledge in digital forensics for forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers. The program equips candidates with the necessary skills to proactively investigate complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks.

Course Focus and Acquired Skills:

- The computer forensic investigation process and the various legal issues involved
- Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner

Types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category

Roles of the first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, and reporting the crime scene

- Setting up a computer forensics lab and the tools involved in it
- Various file systems and how to boot a disk
- Gathering volatile and non-volatile information from Windows
- Data acquisition and duplication rules
- Validation methods and tools required
- Recovering deleted files and deleted partitions in Windows, Mac OS X, and Linux

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- Forensic investigation using AccessData FTK and EnCase
- Steganography and its techniques
- Steganalysis and image file forensics
- Password cracking concepts, tools, and types of password attacks
- Investigating password protected files
- Types of log capturing, log management, time synchronization, and log capturing tools
- Investigating logs, network traffic, wireless attacks, and web attacks
- Tracking emails and investigate email crimes
- Mobile forensics and mobile forensics software and hardware tools
- Writing investigative reports

Course Outline

- **Lesson 1: Computer Forensics in Today's World**
- **Lesson 2 : Computer Forensics Investigation Process**
- **Lesson 3 : Understanding Hard Disks and File Systems**
- **Lesson 4: Data Acquisition and Duplication**
- **Lesson 5: Defeating Anti-Forensics Techniques**
- **Lesson 6: Windows Forensics**
- **Lesson 7: Linux and Mac Forensics**
- **Lesson 8: Network Forensics**
- **Lesson 9: Investigating Web Attacks**
- **Lesson 10 : Dark Web Forensics**
- **Lesson 11: Database Forensics**
- **Lesson 12: Cloud Forensics**
- **Lesson 13 : Investigating Email Crimes**
- **Lesson 14: Malware Forensics**
- **Lesson 15: Mobile Forensics**
- **Lesson 16: IoT Forensics**

Intended Audience

The program is designed for IT professionals involved with information system security, computer forensics, and incident response including:

- Police and other law enforcement personnel
- Defense and Military personnel

- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance, and other professionals
- Government agencies
- IT managers
- Digital Forensics Service Providers

Prerequisites

It is strongly recommended that you attend Certified Ethical Hacker before enrolling into CHFI program.

Follow-On Courses

- CompTIA PenTest+
- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.